One embodiment of the present invention presumes a number of document authors distributed throughout a communication network. Such authors may be individuals, companies, company departments, etc., each representing a distinct and identifiable, e.g., by ID number or the like, member of the author universe. This universe would be supported by a central record repository and would, in essence, constitute the clientele of such an outside time-stamping agency (TSA).

In this particular application, as depicted in FIG. 1 of the drawing, the method entails an author's preparation of a digital document, which may broadly comprise any alphanumeric, audio, or pictorial presentation, and the transmission of the document, preferably in a condensed representative form, to the TSA. The TSA time-stamps the document to create a receipt by adding digital data signifying the current time, concatenates the receipt with the current cryptographic catenation of its prior time stamp receipts, and creates a new catenation from the composite document by means of a deterministic function, such as discussed in greater detail below. The resulting catenate value is then included with time and other identifying data in a document, now a certificate of the temporal existence of the original document, which is transmitted back to the author where it will be held for later use in any required proof of such existence.

To ensure against interception of confidential document information during transmission to the TSA, and to reduce the digital bandwidth required for transmission of an entire document, the author may optionally convert the digital document string to a unique value having vastly condensed digital size by means of a deterministic function which may, for example, be any one of a number of algorithms known in the art as "one-way hash functions". Such an application of hash functions has been described, among others, by Damgard in his discussions on the improvement of security in document signing techniques ("Collision-Free Hash Functions and Public Key Signature Schemes", *Advances in Cryptology—Eurocrypt* '87, Springer-Verlag, LNCS, 1988, Vol. 304, pp. 203–217). In practice of the present invention, however, the "one-way" characteristic typical of a hashing algorithm serves an additional purpose; that is, to provide assurance that the document cannot be secretly revised subsequent to the time the TSA applies its time stamp and incorporates the document into the catenate certificate.

A hashing function provides just such assurance, since at the time a document, such as an author's original work or a composite receipt catenation, is hashed there is created a representative "fingerprint" of its original content from which it is virtually impossible to recover that document. Therefore, the time-stamped document is not susceptible to revision by any adversary of the author. Nor is the author able to apply an issued time-stamp certificate to a revised form of the document, since any change in the original document content, even to the extent of a single word or a single bit of digital data, results in a different document that would hash to a completely different fingerprint value. Although a document cannot be recovered from its representative hash value, a purported original document can nonetheless be proven in the present time-stamping procedure by the fact that a receipt concatenation comprising a true copy of the original document representation will always hash to the same catenate value as is contained in the author's certificate, assuming use of the original hashing algorithm.

Any available deterministic function, e.g. a one-way hash function such as that described by Rivest ("The MD4 Message Digest Algorithm", *Advances in Cryptology—Crypto* '90, Springer-Verlag, LNCS, to appear), incorporated herein by reference, may be used in the present procedure. In the practice of the invention, such a hashing operation is optionally employed by the author to obtain the noted benefit of transmission security, although it might be effected by the TSA if the document were received in plaintext form. In whatever such manner the document content and incorporated time data are fixed against revision, there remains the further step, in order to promote the credibility .of the system, of certifying to the members of an as yet unidentified universe that the receipt was in fact prepared by the TSA, rather than by the author, and that the time indication is correct, i.e., that it has not, for instance, been fraudulently stated by the TSA in collusion with the author.

To satisfy these concerns, the TSA maintains a record of its sequential time-stamping transactions by adding each new receipt to its current catenation and applying its deterministic function, e.g. hashing, the composite to obtain a new catenation. This catenation, itself a value resulting from the hashing process, is included on the receipt or certificate returned to the author and serves to certify the indicated time stamp. Confirmation of the certificate at a later time involves rehashing the combination of the author's time receipt and the next previous catenate value in the TSA records. The resulting generation of the author's catenate certificate value proves to the author and to the universe at large that the certificate originated with the TSA. This result also proves the veracity of the time-stamp itself, since all original elements of the original receipt must be repeated in order to again generate, by the hashing function, the original catenate certificate value.

The process of the invention relies upon the relatively continuous flow of documents from the universe of authors through the facilities of the TSA. For each given processed document D_k, from an author, A_k, the TSA generates a time-stamp receipt which includes, for example, a sequential receipt transaction number, r_k, the identity of the author, for example by ID number ID_k, or the like, a digital representation, e.g. the hash, H_k, of the document, and the current time, t_k. The TSA then includes these receipt data, or any representative part thereof, with the catenate certificate value, C_{k-1}, of the immediately preceding processed document D_{k-1}, of author, A_{k-1}, thereby bounding the time-stamp of document D_k, by the independently established earlier receipt time, t_{k-1}.

The composite data string, r_k, ID_k, H_k, t_k, C_{k-1}), is then hashed to a new catenate value, C_k, that is entered with transaction number, r_k, in the records of the TSA, and is also transmitted to A_k, as the catenate certificate value, with the time-stamp receipt data. In like manner, a certificate value derived from the hashing of C_k with time stamp elements of the receipt for document D_{k+1}, would be transmitted to author, A_{k+1}. Thus, each of the time-stamped catenate certificates issued by the TSA is fixed in the continuum of time and none can be falsely prepared by the TSA, since any attempt to regenerate a catenate certificate number from a hash with the next prior certificate would reveal the discrepancy.